SUBOPTIMUM DECODING OF BLOCK CODES

Technical Report

to

NASA

Goddard Space Flight Center

Greenbelt, Maryland 20771

Grant Number NAG 5-931

Report Number NASA 91-004

Shu Lin

Principal Investigator

Department of Electrical Engineering

University of Hawaii at Manoa

Honolulu, Hawaii 96822

October 15, 1991

Suboptimum Decoding of Block Codes [1]

Tadao Kasami
Faculty of Engineering Science
Osaka University
Toyonaka, Osaka 560, Japan

Shu Lin
Department of Electrical Engineering
University of Hawaii at Manoa
Honolulu, Hawaii 96822 , U.S.A

ABSTRACT

This paper investigates a class of decomposable codes, their distance and structural properties. It is shown that this class includes several classes of well known and efficient codes as subclasses. Several methods for constructing decomposable codes or decomposing codes are presented. A two-stage soft decision decoding scheme for decomposable codes, their translates or unions of translates is devised. This two-stage soft-decision decoding is suboptimum, and provides an excellent trade-off between the error performance and decoding complexity for codes of moderate and long block length.

1. Introduction

To decode a long block code with maximum likelihood decoding is practically impossible because the decoder complexity is simply **enormous**, However, if a code can be **decomposed** into **constituent codes** with **smaller dimension** and **simpler structure,** it is possible to devise a practical and yet efficient scheme to decode the code as follows: (1) The constituent codes are decoded sequentially in multiple stages. The decoded codeword of one constituent code at one stage is passed to the next stage for decoding the next constituent code; and (2) From the decoded constituent codewords, we form the overall decoded codeword based on the code structure. This type of decoding is **not optimum** even if the decoding of each constituent code is optimum. It is a **suboptimum** decoding scheme. However, this decoding scheme **reduces** the overall decoding complexity **drastically** comparing with the optimum decoding of the overall code. This is because the constituent codes are **smaller** in dimension and **much simpler** in decoding complexity. If the constituent codes have the right structure (such as **trellis structure**) and the decoding scheme is devised properly, an excellent **trade-off** between the error performance and decoding complexity can be attained.

In this paper, we first define a class of decomposable codes, and show that several classes of good known codes are decomposable. Several methods for constructing decomposable or decomposing codes are presented. Then a two-stage suboptimum decoding scheme is devised for decomposable codes, their translates and unions of their translates. This suboptimum decoding scheme reduces the overall decoding complexity drastically comparing with the single-stage optimum decoding for the same decomposable code while maintains excellent performance. The error performance of some specific decomposable codes based on the proposed two-stage suboptimum decoding is evaluated and simulated. It is shown that the proposed two-stage suboptimum decoding achieves excellent error performance with reduced decoding complexity.

2. Decomposable Codes

Let L be a finite set of symbols on which an **addition** "+", a **substraction** "−", and a distance measure $d(\cdot,\cdot)$ (**Euclidean** or **Hamming**) are defined. Let 0 denote the **zero element** of L. The distance measure $d(u,v)$ between two elements, u and v, in L is assumed to satisfy the following properties: (1) $d(u,v) = 0$ if and only if $u = v$, and (2) $d(u,v) = d(v,u)$. For the binary case, L is defined as the binary set $\{0,1\}$, the distance measure d is given by $d(0,1) \triangleq 1$, and the "+" on L is defined as the modulo-2 addition. For a 2^ℓ-ary PSK signal set S, L is simply defined as the set of all binary label strings of length ℓ for the signal points in S. In this case, the addition "+" means the **bit-wise** modulo-2 addition.

For two j-tuples, $\mathbf{u} = (u_1, u_2, \cdots, u_n)$ and $\mathbf{v} = (v_1, v_2, \cdots, v_n)$ over L, let $\mathbf{u} + \mathbf{v}$ and $d(\mathbf{u}, \mathbf{v})$ be defined as,

$$\mathbf{u} + \mathbf{v} = (u_1 + v_1, u_2 + v_2, \cdots, u_j + v_j) \tag{2.1}$$

$$d(\bar{\mathbf{u}}, \bar{\mathbf{v}}) = \sum_{i=1}^{j} d(u_i, v_i) \tag{2.2}$$

respectively. For a block code C over L, let $d[C]$ denote the minimum distance of C with respect to the distance measure d.

For block codes C and C' of the same length over L, let $C + C'$ denote the set $\{\mathbf{u} + \mathbf{v} : \mathbf{u} \in C \text{ and } \mathbf{v} \in C'\}$. If C' consists of a single codeword $\mathbf{v}$, then $C + \{\mathbf{v}\}$ is called a **translate** of C [1]. If for any two different codewords $\mathbf{u}$ and $\mathbf{u}'$ in C and any two different codeword $\mathbf{v}$ and $\mathbf{v}' \in C'$, $\mathbf{u} + \mathbf{v} \neq \mathbf{u}' + \mathbf{v}'$,then C and C' are said to be "**independent**". If a code is **closed** under the component-wise addition "+" and subtraction "−", the code is said to be additive. For an additive code C and its **supercode** C' which is a set of cosets of C, let $[C'/C]$ denote the set of **representatives** of cosets of C in C'. For C itself, the all-zero n-tuple $\mathbf{0}$ is always chosen as its representative.

Let m be a positive integer, and let n be a positive inetger divisible by m. For a code C of length n over L, C is said to be **decomposable** with respect to U_1 and U_2 if there exist independent codes U_1 and U_2 of length m over L, and codes C_1 and C_2 of length n over L such that : $(A1)$ $C_1 \subseteq (U_1)^{n/m}$ $(A2)$ $C_2 \subseteq (U_2)^{n/m}$, and $(A3)$ $C = C_1 + C_2 \triangleq \{\bar{\mathbf{u}} + \bar{\mathbf{v}} : \bar{\mathbf{u}} \in C_1 \text{ and } \bar{\mathbf{v}} \in C_2\}$, where $A^{n/m}$ denotes the following Cartesian product of A,

$$A^{n/m} = \underbrace{A \times A \times \cdots \times A}_{n/m}.$$

For $\mathbf{u}$ and $\mathbf{u}'$ in U_1 and $\mathbf{v}$ and $\mathbf{v}'$ in U_2, let $d^{(1)}_{U_1,U_2}(\mathbf{u}, \mathbf{u}')$ and $d^{(2)}_{U_1,U_2}(\mathbf{v}, \mathbf{v}')$ be defined as follows:

$$d^{(1)}_{U_1,U_2}(\mathbf{u}, \mathbf{u}') = \min\{d(\mathbf{u} + \mathbf{v}, \mathbf{u}' + \mathbf{v}') : \mathbf{v} \text{ and } \mathbf{v}' \text{ in } U_2\} \tag{2.3}$$

$$d^{(2)}_{U_1,U_2}(\mathbf{v}, \mathbf{v}') = \min\{d(\mathbf{u} + \mathbf{v}, \mathbf{u} + \mathbf{v}') : \mathbf{u} \text{ in } U_1\} \tag{2.4}$$

Clearly $d^{(1)}_{U_1,U_2}(\mathbf{u}, \mathbf{u}) = d^{(2)}_{U_1,U_2}(\mathbf{v}, \mathbf{v}) = 0$, $d^{(1)}_{U_1,U_2}(\mathbf{u}, \mathbf{u}') = d^{(1)}_{U_1,U_2}(\mathbf{u}', \mathbf{u})$ and $d^{(2)}_{U_1,U_2}(\mathbf{v}, \mathbf{v}') = d^{(2)}_{U_1,U_2}(\mathbf{v}', \mathbf{v})$.

For simpicity, we regard an n-tuple over L as a n/m tuple over L^m, the set of all m-tuple over L, and vice versa. We also consider a code of length n over L as a code of length n/m over L^m and vice versa. For two codewords , $\mathbf{x} = (\mathbf{x}_1, \mathbf{x}_2, \cdots, \mathbf{x}_{n/m})$ and $\mathbf{y} = (\mathbf{y}_1, \mathbf{y}_2, \cdots, \mathbf{y}_{n/m})$ in C_i with $\mathbf{x}_j$ and $\mathbf{y}_j$ in U_i for $1 \leq i \leq 2$ and $1 \leq j \leq n/m$, define the distance between $\mathbf{x}$ and $\mathbf{y}$ based on the distance measure $d^{(i)}_{U_1,U_2}(\cdot, \cdot)$ given by (2.3) or (2.4) as follows:

$$d^{(i)}_{U_1,U_2}(\mathbf{x}, \mathbf{y}) = \sum_{j=1}^{n/m} d^{(i)}_{U_1,U_2}(\mathbf{x}_j, \mathbf{y}_j). \tag{2.5}$$

Then the minimum distance of C_i based on the distance measure given by (2.3) or (2.4) is defined as follows:

$$d^{(i)}_{U_1,U_2}[C_i] \triangleq \{d^{(i)}_{U_1,U_2}(\mathbf{x}, \mathbf{y}) : \mathbf{x}, \mathbf{y} \in C_i\}. \tag{2.6}$$

Lemma 1: The minimum distance $D[C]$ of a decomposable code $C(= C_1 + C_2)$ with respect to U_1 and U_2 is lower bounded by :

$$d[C] \geq \min\{d^{(1)}_{U_1,U_2}[C_1], d^{(2)}_{U_1,U_2}[C_2]\}. \tag{2.7}$$

If the equality in (2.7) holds, then C is said to be **strictly** decomposable.

It is clear that given two block codes C_1 and C_2 over L which satisfy the conditions (A1) and (A2), we can form a decomposable code $C = C_1 + C_2$ over L. In the following, we use some examples to demonstrate how to construct decomposable codes and to show that some known codes are decomposable. Hereafter, the following notations are used: (1) V_n denotes the set of all binary n-tuples $(= \{0,1\}^n)$; (2) P_n denotes the $(n, n-1)$ linear code which consists of all the even-weight binary n-tuples; (3) $RM_{i,j}$ denotes the j-th order Reed-Muller (RM) code of length $n = 2^i$; and (4) For a code C, $C^\perp$ denotes the dual code of C. $P_n^\perp$ consists of the all-zero n-tuple $\mathbf{0}$ and the all-one n-tuple $\mathbf{1}$.

Example 1 : Consider a binary case where $m = 2$, $U_1 = \{(0,0),(0,1)\}, U_2 = P_2 = \{(0,0),(1,1)\}$ and $U_1 + U_2 = \{0,1\}^2$. Then $d^{(1)}_{U_1,U_2}((0,0),(0,1)) = d((0,0),(0,1)) = d(0,1)$ and $d^{(2)}_{U_1,U_2}((0,0),(1,1)) = d((0,0),(1,1)) = 2d(0,1)$. Let n be an even positive integer. For a binary $n/2-$ tuple, $\mathbf{u} = (u_1, u_2, \cdots u_{n/2})$, let $\phi_1(\mathbf{u})$ and $\phi_2(\mathbf{u})$ denote two n-tuples obtained from $\mathbf{u}$ as follows : (1) $\phi_1(\mathbf{u})$ is obtained from $\mathbf{u}$ by substituting 00 and 01 for 0 and 1 in $\mathbf{u}$ respectively. (2) $\phi_2(\mathbf{u})$ is obtained from $\mathbf{u}$ by substituting 00 and 11 for 0 and 1 in $\mathbf{u}$ respectively. Let $\mathbf{X}$ and $\mathbf{Y}$ be two linear binary block codes of length $n/2$. Define the following two linear binary codes of length n : $C_1 \triangleq \phi_1[\mathbf{X}] = \{\phi_1(\mathbf{x}) : \mathbf{x} \in \mathbf{X}\}$ and $C_2 \triangleq \phi_2[\mathbf{Y}] = \{\phi_2(\mathbf{y}) : \mathbf{y} \in \mathbf{Y}\}$. Then $C = C_1 + C_2$ is decomposable with respect to $U_1 = \{(0,0),(0,1)\}$ and $U_2 = \{(0,0),(1,1)\}$. The above construction of a decomposable code with respect to $U_1 = \{(0,0), (0,1)\}$ and $U_2 = \{(0,0),(1,1)\}$ is simply a **permutation** of the $|\mathbf{u}|\mathbf{u}+\mathbf{v}|$-construction of codes. Therefore, codes obtained from the $|\mathbf{u}|\mathbf{u}+\mathbf{v}|$-construction are decomposable with respect to $U_1 = \{(0,0),(0,1)\}$ and $U_2 = \{(0,0),(1,1)\}$ after a certain permutation.

Now we show that RM codes are decomposable with respect to $U_1 = \{(0,0), (0,1)\}$ and $U_2 = \{(0,0),(1,1)\}$. Let $C_1 = \phi_1[RM_{m-1,r-1}]$ and $C_2 = \phi_2[RM_{m-1,r}]$. It is known [1] that

$$RM_{m,r} = \phi_1[RM_{m-1,r-1}] + \phi_2[RM_{m-1,r}]. \tag{2.8}$$

From (2.3) and (2.4), we find that $d^{(1)}_{U_1,U_2}[C_1] = 2^{m-r}$ and $d^{(2)}_{U_1,U_2}[C_2] = 2^{m-r}$. Since $d(RM_{m,r}) = 2^{m-r}$, the equality of (2.7) holds. Therefore Reed-Muller codes are decomposable with respect to $U_1 = \{(0,0),(0,1)\}$ and $U_2 = \{(0,0),(1,1)\}$.

Example 2 : Consider a binary case where $m = 4$, $U_{11} = \{(0,0),(0,1)\}^2, U_{12} = \{(0,0,0,0),(0,0,1,1)\}$, $U_1 = U_{11} + U_{12}$ and $U_2 = P_4^\perp$. Let C'_{11} be a block binary code of length $n/2$ and and minimum Hamming distance δ_{11}, C'_{12} be a binary block code of length $n/4$ and minimum Hamming distance δ_{12}, and C'_2 be a binary block code of length $n/4$ and minimum Hamming distance δ_2. For a binary j-tuple $\mathbf{u}$, let $\phi_2\phi_1(\mathbf{u})$ (or $\phi_2\phi_2(\mathbf{u})$) denote the $4j$-tuple derived from $\mathbf{u}$ by substituting $(0,0,0,0)$ for each component 0 and

$(0,0,1,1)$ (or $(1,1,1,1)$) for each component 1. Let C_{11}, C_{12}, C_1 and C_2 be defined as follows : (1) $C_{11} \triangleq \phi_1[C'_{11}]$; (2) $C_{12} \triangleq \phi_2\phi_1[C'_{12}]$; (3) $C_1 \triangleq C_{11} + C_{12}$; and (4) $C_2 \triangleq \phi_2\phi_2[C'_2]$; where ϕ_1 and ϕ_2 are defined in Example 1, and for a mapping f and a block code C', $f[C'] \triangleq \{f(\mathbf{v}) : \mathbf{v} \in C'\}$. Then $C = C_1 + C_2$ is decomposable with respect to U_1 and U_2. It can be shown that $d[C] \geq \min\{\delta_{11}, 2\delta_{12}, 4\delta_2\}$. If C'_{11}, C'_{12} and C'_2 contain the all-zero n-tuple $\mathbf{0}$, then $d[C] = \min\{\delta_{11}, 2\delta_{12}, 4\delta_2\}$, and C is strictly decomposable.

As an example, consider $RM_{m,r}$ with $r \geq 2$. From (2.8), we see that $RM_{m,r}$ is decomposable with respect to U_1 and U_2 as follows:

$$RM_{m,r} = (\phi_1[RM_{m-1,r-1}] + \phi_2\phi_1[RM_{m-2,r-1}]) + \phi_2\phi_2[RM_{m-2,r}]. \tag{2.9}$$

In fact, C_1 is decomposable with respect to $U_{11} + U_{12}$.

Besides RM codes, multi-level concatenated codes [2] and multilevel modulation codes [3-5] are also decomposable. Some primitive BCH codes are union of a decomposable code and its translates.

3. Two-Stage Decoding

In this section, we present a two-stage suboptimum decoding for a decomposable code, $C = C_1 + C_2$, over L with respect to U_1 and U_2 which achieves the distance $\min\{d^{(1)}_{U_1,U_2}[C_1], d^{(2)}_{U_1,U_2}[C_2]\}$. The first stage is for decoding C_1 based on the distance measure $d^{(1)}_{U_1,U_2}(\cdot,\cdot)$, and the second stage decoding is for decoding C_2 based on the distance measure $d^{(2)}_{U_1,U_2}(\cdot,\cdot)$.

Let $C = C_1 + C_2$ be a decomposable code of length n over L with respect to U_1 and U_2 over L^m, where n is divisible by m. Suppose C is used for error control over an AWGN channel. Assume that all the codewords in C are equally likely to be transmitted. For $v \in L$, let $s(v)$ denote the signal point in R^h represented by v, where R^h denotes the set of all h-tuples of real numbers, and for a j-tuple $\mathbf{v} = (v_1, v_2, \cdots, v_j)$ over L, let $s(\mathbf{v})$ denote the j-tuple, $(s(v_1), s(v_2), \cdots, s(v_j))$. For z and z' in R^h, let $\| z - z' \|$ denote the Euclidean distance between z and z'. For j-tuples $\mathbf{z} = (z_1, z_2, \cdots, z_j)$ and $\mathbf{z}' = (z'_1, z'_2, \cdots, z'_j)$ over R^h, let $\| \mathbf{z} - \mathbf{z}' \|^2$ be defined as $\sum_{i=1}^{j} \| z_i - z'_i \|^2$, the squared Euclidean distance between $\mathbf{z}$ and $\mathbf{z}'$. The distance measure d on L is assumed to satisfy the condition that for u and v in L, $\| s(u) - s(v) \|^2 \geq d(u,v)$. Suppose that (1) for $u \in L$, a one-to-one mapping T_u from R^h to R^h which preserves the squared Euclidean distance is defined, and (2) for u and v in L, $s(v-u) = T_u(s(v))$. Suppose a codeword in C is transmitted. Let $\mathbf{z} = (z_1, z_2, \cdots, z_n)$ be the received vector over R^h. A two-stage decoding procedure **(D)** for C can be formulated as follows:

(D1) Decode $\mathbf{z}$ into a codeword in C_1. Let $\mathbf{u} = (u_1, u_2, \cdots, u_n)$ be the decoded codeword in C_1.

(D2) From $\mathbf{u}$, we form the following vector based on the mapping $T_u(\cdot)$:

$$T_{\mathbf{u}}(\mathbf{z}) = (T_{u_1}(z_1), T_{u_2}(z_2), \cdots, T_{u_n}(z_n))$$

Decode $T_{\mathbf{u}}(\mathbf{z})$ into a codeword in C_2. Let $\mathbf{v} = (v_1, v_2, \cdots, v_n)$ be the decoded codeword .

(D3) The decoded codeword is given by $\mathbf{u} + \mathbf{v} = (u_1 + v_1, u_2 + v_2, \cdots, u_n + v_n)$.

The decodings of C_1 and C_2 may be either **soft-decision** or **hard-decision, maximum likelihood** or **bounded distance.** We may take advantage of the structure of C_1, C_2, U_1 and U_2 to simplify the decodings. Since the dimensions of C_1 and C_2 are **smaller** than that of C and U_1 and U_2 are much shorter than C, the above two-step decoding may result in a **drastic reduction** in decoding complexity .

Suppose both C_1 and C_2 have n/m-section trellis diagrams, each branch in the trellis diagram for C_1 is a codeword in U_1 and each branch in the trellis diagram for C_2 is a codeword in U_2. Then a soft-decision **(SD)** decoding procedure for the above two-stage decoding can be devised as follows:

(SD1) Divide the received vector $\mathbf{z}$ into n/m sections, $\mathbf{z}_i$, for $1 \leq i \leq n/m$, with each section containing m consecutive components of $\mathbf{z}$. Using the trellis diagram for C_1 and the Viterbi algorithm, decode the n/m-tuple $\mathbf{z} = (\mathbf{z}_1, \mathbf{z}_2, \cdots, \mathbf{z}_{n/m})$ into a codeword $\mathbf{u}$ in C_1 . The branch metrics in the i-th section of the trellis diagram are

$$\min_{\mathbf{v} \in \{\mathbf{r}\} + U_2} \|\mathbf{z}_i - s(\mathbf{v})\| \tag{3.1}$$

for each $\mathbf{r} \in U_1$. If U_2 has a trellis diagram, the branch metric of (3.1) can be computed by using a trellis diagram for $\{\mathbf{r}\} + U_2$.

(SD2) Let $\mathbf{u} = (u_1, u_2, \cdots, u_n)$ be the decoded codeword in C_1 at step **SD1** . Form the vector

$$T_{\mathbf{u}}(\mathbf{z}) = (T_{u_1}(z_1), T_{u_2}(z_2), \cdots, T_{u_n}(z_n)),$$

and decode it into a codeword $\mathbf{u}$ in C_2 based on the trellis diagram for C_2 using the Viterbi algorithm. To compute the branch metrics at each trellis section, we divide $T_{\mathbf{u}}(\mathbf{z})$ into n/m sections, $T_{\mathbf{u}}(\mathbf{z}_i)$ for $1 \leq i \leq n/m$. The branch metrics in the i-th section of the trellis diagram for C_2 are computed based on $\|T_{\mathbf{u}}(\mathbf{z}_i) - s(\mathbf{v})\|$ with $\mathbf{v} \in U_2$.

(SD3) The decoded codeword in C is given by $\mathbf{u} + \mathbf{v}$.

It is clear that if C_2 is decomposable, C_2 can be decoded in two stages. The decoding procedure **(D)** can be applied recursively.

Note that the two-stage soft-decision maximum likelihood decoding is a suboptimum decoding. In the next section, we will show that this suboptimum decoding achieves excellent error performance comparing with the single-stage optimum (soft-decision maximum likelihood) decoding while reduces the overall decoding complexity drastically. It is clear that a two-stage hard-decision decoding can be devised.

The proposed two-stage decoding is applicable to any code which is a translate of a decomposable code. If a code C is a set of translates of a decomposable code, the decoding can be carried out as follows: (1) Decode the received vector $\mathbf{z}$ into a codeword in each translate by the above two-stage decoding ; and (2) Choose the **most probable** one among all the decoded words as the final decoded codeword.

Sufficient conditions under which the proposed two-stage decoding procedure result in a correct decoding for an AWGN channel, are given in Lemma 2.

Lemma 2 : Using the two-stage soft decision maximum likelihood decoding, if a codeword $\mathbf{w} \in C$ is transmitted and $\mathbf{z}$ is received such that

$$\| \mathbf{z} - s(\mathbf{w}) \|^2 < \min\{d^{(1)}_{U_1,U_2}[C_1], d^{(2)}_{U_1,U_2}[C_2]\}/4$$

then $\mathbf{z}$ is correctly decoded into $\mathbf{w}$.

4. Performance

In the following, we use three examples to demonstrate that the proposed decoding of decomposable codes indeed reduces the decoding complexity drastically while maintains excellent error performance. A decomposable code may be decomposed in different ways. Different decompositions result in different error performance and decoding complexities. In general, the error performance of the first stage decoding has dominant effect on the overall error performance and the first constituent code should be chosen as large as possible within allowable decoding complexity.

Example 3. : In Example 1, we showed that the r-th order RM code $C = RM_{m,r}$ of length 2^m and minimum distance 2^{m-r} is strictly decomposable with respect to $U_1 = \{(0,0),(0,1)\}$ and $U_2 = \{(0,0),(1,1)\}$. The constituent codes of $C = RM_{m,r}$ are: $C_1 = \phi_1[RM_{m-1,r-1}]$ and $C_2 = \phi_2[RM_{m-1,r}]$. $RM_{m-1,r-1}$ and $RM_{m-1,r}$ have 4-section trellis diagrams with $2^{\binom{m-2}{r-1}}$ states and $2^{\binom{m-2}{r}}$ states respectively[6]. It is easy to see that C_1 and C_2 also have 4-section trellis diagrams with $2^{\binom{m-2}{r-1}}$ states and $2^{\binom{m-2}{r}}$ states respectively. The RM code $C = RM_{m,r}$ has a 4-section trellis with $2^{\binom{m-1}{r}}$ states. If we decode $C = RM_{m,r}$ with the optimum decoding using Viterbi algorithm, the state complexity of the Viterbi decoder is $2^{\binom{m-1}{r}}$. However, if we decode $C = RM_{m,r}$ with the proposed two-stage suboptimum decoding algorithm, the overall state complexity of the Viterbi decoder is $2^{\binom{m-2}{r}} + 2^{\binom{m-2}{r-1}}$ which is **much smaller** than $2^{\binom{m-1}{r}}$, the state complexity of the 4-section trellis diagram for the overall code $C = RM_{m,r}$ for $m \geq 5$. For example, let $m = 6$ and $r = 2$. Then $C = RM_{6,2}$ is a (64,22) code which has a 4-section trellis diagram with $2^{\binom{5}{2}} = 1024$ states. However, its constituent codes, $C_1 = \phi_1[RM_{5,1}]$ and $C_2 = \phi_2[RM_{5,2}]$, have 4-section trellis diagrams with $2^{\binom{4}{1}} = 16$ states and $2^{\binom{4}{2}} = 64$ states respectively. Using the two-stage suboptimum decoding, the total state complexity of a Viterbi decoder is 80 which is much smaller than the state complexity 1024 for the single-stage optimum decoding for $C = RM_{6,2}$. The code $C = RM_{6,2}$ has minimum distance 16, which is comparable to a rate - 1/3 optimum convolutional code of constraint length 8 and free distance 16 [7]. To decode this convolutional code with the Viterbi algorithm, a Viterbi decoder of 128 states is needed.

The error performance of the RM code $C = RM_{6,2}$ with the proposed two-stage suboptimum soft-decision decoding based on the above decomposition,denoted $2s_1$, is shown in **Figure 1**. We see that it achieves 5.1db coding gain over the uncoded BPSK at block error rate 10^{-5}. Figure 1 also shows simulation results $p^{(2)}_{ic,s}[2s_1]$ on the probability that the first stage decoding is correct but the second stage decoding is incorrect. Compared with the simulation results $p_{ic,s}[2s_1]$ on the overall error probability, $p^{(2)}_{ic,s}[2s_1]$ is very small. This fact suggests to choose a supercode of $\phi_1[$ RM$_{5,1}]$ as the first constituent if the decoding complexity is allowable. By applying the decomposition shown in Example 2 to RM$_{6,2}$, we have $C_1 \triangleq \phi_1[RM_{5,1}]+\phi_1\phi_2[RM_{4,1}]$ and $C_2 \triangleq \phi_2\phi_2[RM_{4,2}]$ as the first and second constituent codes, respectively. C_1 and C_2 have 4-section trellis diagrams with 128 states and 8 states, respectively. Note that the first consituent code in the decomposition contains the first constituent code of the former decomposition as a small subcode. The error performance of $RM_{6,2}$ with this decomposition, denoted $2s_2$, is shown in Figure 1. It achieves 5.6dB coding gain over the uncoded BPSK at block error rate 10^{-5}. Figure 1 also shows simulation results , denoted $p_{ic,s}[1s]$, and union upper bounds, denoted $\overline{p_{ic}}$ $[1s]$, on the probability of incorrect decoding for the single stage optimum decoding. We see that the coding losses of the two-stage suboptimum decodings based on decompositions $2s_1$ and $2s_2$ from the single-stage optimum decoding are about 1.0dB and 0.5dB, respectively, at the block error rate 10^{-5}. However there is a big reduction in decoding complexity.

It is known that an extended and permuted BCH code of length 2^m and minimum distance 2^{m-r} contains the r-th order Reed-Muller code RM$_{m,r}$ as a proper subcode[1,7]. As a result, this extended and permuted BCH code is a union of cosets (or translates) of the Reed-Muller code RM$_{m,r}$. Since RM$_{m,r}$ is decomposable and has relatively simple trellis structure, this extended and permuted BCH code can be decoded with the proposed suboptimum soft-decision two-stage decoding. First we decode the received n-tuple $\mathbf{z}$ into a codeword in each translate of the $RM_{m,r}$ code by the proposed two-stage decoding. Then we choose the most probable one among all the decoded words as the final decoded codeword. All the translates of the $RM_{m,r}$ code have trellis diagrams isomorphic to that of the $RM_{m,r}$ code. Let K be the total number of translates of $RM_{m,r}$ (including $RM_{m,r}$ itself). If K is not too big, it is possible to implement K separate but identical Viterbi decoders to decode the K translates of $RM_{m,r}$ in parallel. This definitely speeds up the decoding process.

Example 4: Let C be the extended and permuted $(64, 24)$ BCH code whose complexity of trellis structure has been analysed in [8]. C contains the $(64, 22)$ second order Reed-Muller code as a proper subcode. There are 4 cosets in C modulo $RM_{6,2}$. The coset code $[C/RM_{6,2}]$ is generated by the two codewords $\mathbf{g_1}$ and $\mathbf{g_2}$ which can be determined [8]. Each coset of C modulo $RM_{6,2}$ can be decomposed into two constituent codes, C_1 and C_2, either in the form given in Example 1 (denoted $2s_1$) or in the form given in Example 2 (denoted $2s_2$). The two constituent codes, C_1 and C_2, have a 4-section trellis diagrams with 16 states and 64 states or 128 states and 8 states, respectively. Hence each coset can be decoded with the suboptimum soft-decision two-stage decoding with two Viterbi decoders, one with 16 states (or 128 states) and the other with 64 states (or 8 states). The overall decoder for the $(64, 24)$ extended and permuted BCH code consists of 4 separate two-stage decoders. These four decoders process the received 64-tuple in parallel. The total number of states for the

overall decoder is 320 (or 544). The error performance of this BCH code with suboptimum soft-decision two-stage decoding based on the decomposition $2s_1$ is simulated and shown in **Figure 2**. We see that it achieves 5.4 dB coding gain over the uncoded BPSK at block error rate 10^{-5}, which compares favorably with the rate-1/3 Odenwalter convolutional code of constraint length 8 and free distance 16. If each coset of the $(64, 24)$ extended BCH code modulo $RM_{6,2}$ is decoded with one-stage optimum decoding, four 1024-state Viterbi decoders are needed, one for each coset. This amounts to a total of 4096 states which is much greater than the number of states (320 or 544) in a two stage decoding as described above.

Example 5 : Let C be the extended and permuted $(64, 45)$ BCH code whose complexity of trellis structure has been analyzed in [8]. C includes $RM_{6,3}$, a $(64, 42)$ code, as a subcode. $[C/RM_{6,3}]$ consists of eight cosets. Each coset can be decomposed into two constituent codes, C_1 and C_2 have 4-section trellis diagrams with 64 states and 16 states, respectively. Hence each coset can be decoded with the suboptimum soft-decision two-stage decoding with two Viterbi decoders, one with 16 states and the other with 64 states. The overall decoder for the $(64, 45)$ extended and permuted BCH code consists of 8 separate two-stage decoders. These 8 decoders process the received 64-tuple in parallel. The total number of states for the overall decoder is 640. The error performance of the BCH code with suboptimum soft-decision two-stage decoding based on the above decomposition, denoted $2s_1$, is simulated and shown in Figure 3. We see that it achieves 5.4dB coding gain over the uncoded BPSK at block error rate 10^{-5}. If each coset of the $(64, 45)$ extended BCH code modulo $RM_{6,3}$ is decoded with one-stage optimum decoding, eight 1024-state Viterbi decoders are needed, one for each coset. In this case, the total number of states is 8192 which is much greater than that of the two-stage decoding described above (640 states).

From the above three examples, we see that the proposed code decomposition and two-stage suboptimum decoding achieves excellent reduction in decoding complexity.

5. Conclusion

In this paper, we have shown that code decomposition with multi-stage suboptimum decoding achieves excellent error performance with a drastic reduction in decoding complexity. This finding may have an impact on the future designs of error control systems for reliable data communications. For future work, we should focus in searching efficient decomposable codes with simple trellis structure so that soft-decision Viterbi decoding can be applied.

Refrences

1. F.J. MacWilliams and N.J.A. Sloane, *The Theory of Error-Correcting Codes*, North-Holland, 1977.

2. V. A. Zinoviev, "Generalized Concatenated Codes," *Problemy peredachi Informatsii*, Vol. 12, No. 1, pp. 5-15, 1976.

3. H. Imai and S. Hirakawa, "A New Multilevel Coding Method Using Error Correcting Codes," *IEEE Trans. on Information Theory*, Vol. IT-23, No. 3, pp. 371-376, May 1977.

4. V.V. Ginzburg, " Multidimensional Signals for a Continuous Channel ," *Problemy Peredachi Informatsii*, Vol. 20, No. 1, pp. 28-46, 1984.

5. T. Kasami, T. Takata, T. Fujiwara, and S. Lin, "On Multi-Level Block Modulation Codes," *IEEE Trans. on Information Theory*, Vol. IT-37, No. 4, July 1991.

6. G.D. Forney, Jr., "Coset Codes I: Introduction and Geometrical Classification," *IEEE Trans. on Information Theory*, Vol. IT-34, pp. 1123-1151, September 1988, Part II.

7. S. Lin and D.J. Costello, Jr., *Error Control Coding: Fundamentals and Applications*, Prentice-Hall, Englewood Cliffs, New Jersey, 1983.

8. T. Kasami, T. Takata, T. Fujiwara, and S. Lin,"Representation of Codewords of a Cyclic Code by Boolean Polynomials and Its Application to Trellis Diagram Construction," *Preceedings of the 12th Symposium on Information Theory and Its Applications*, Inuyama, Japan, December 6-9, 1989.

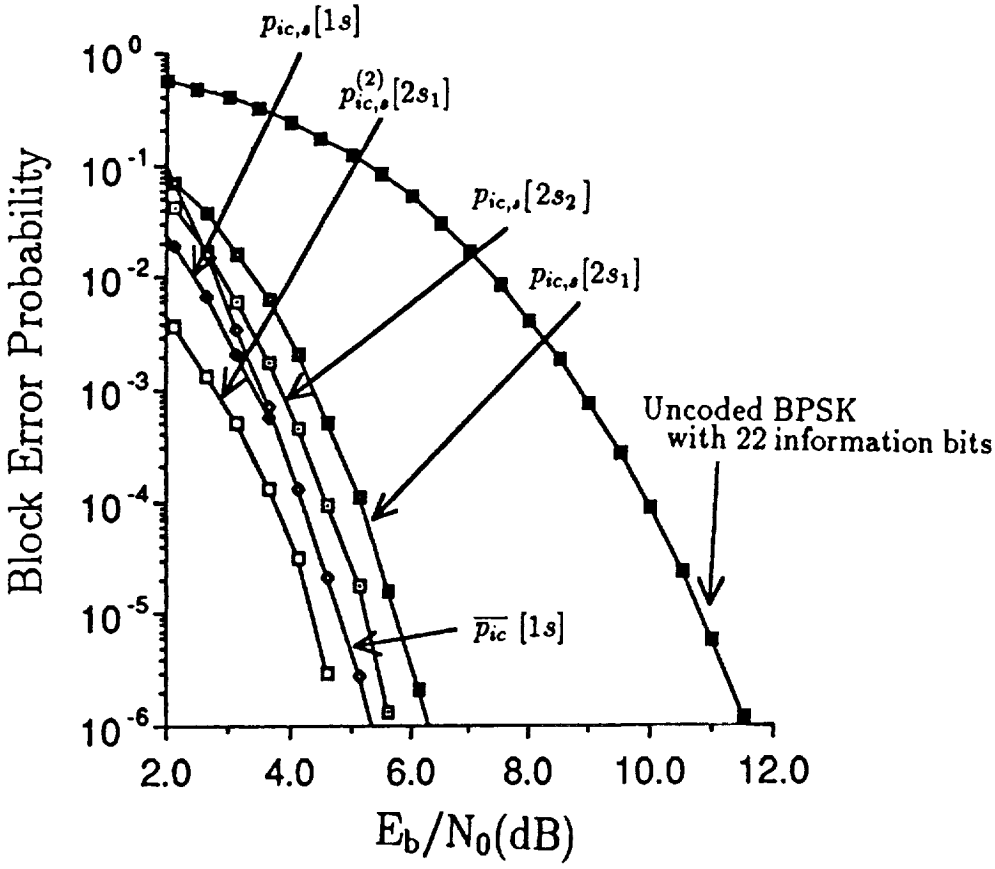

Figure 1. Error performance of $RM_{6,2}$

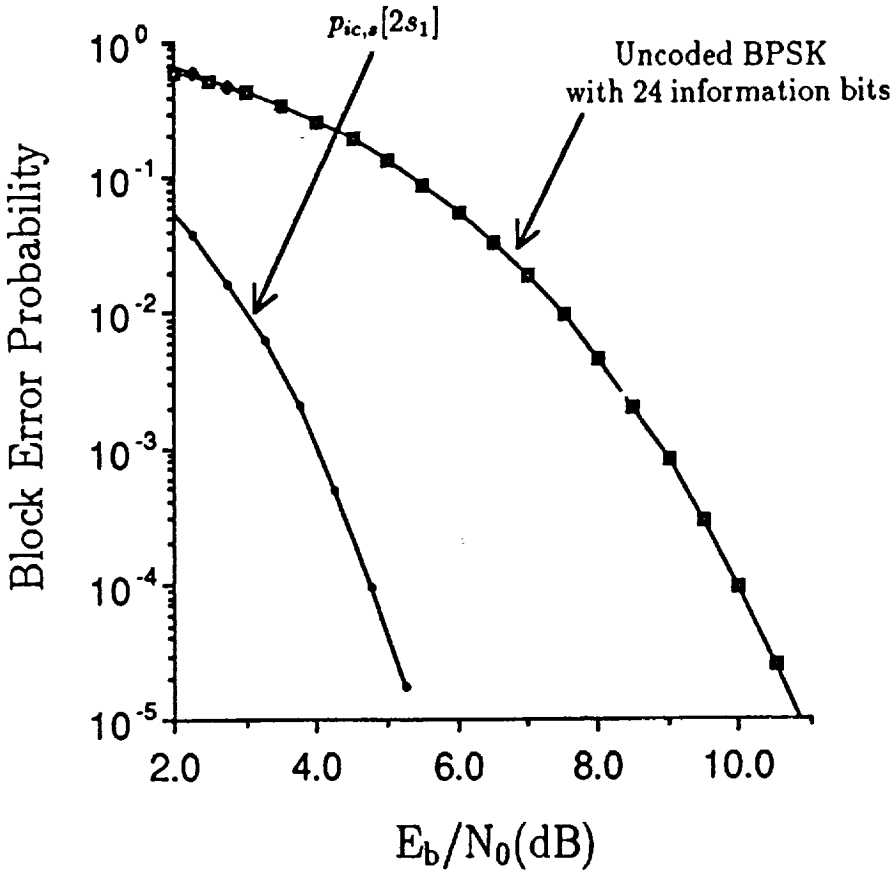

Figure 2. Error performance of extended and permuted (64,24)BCH

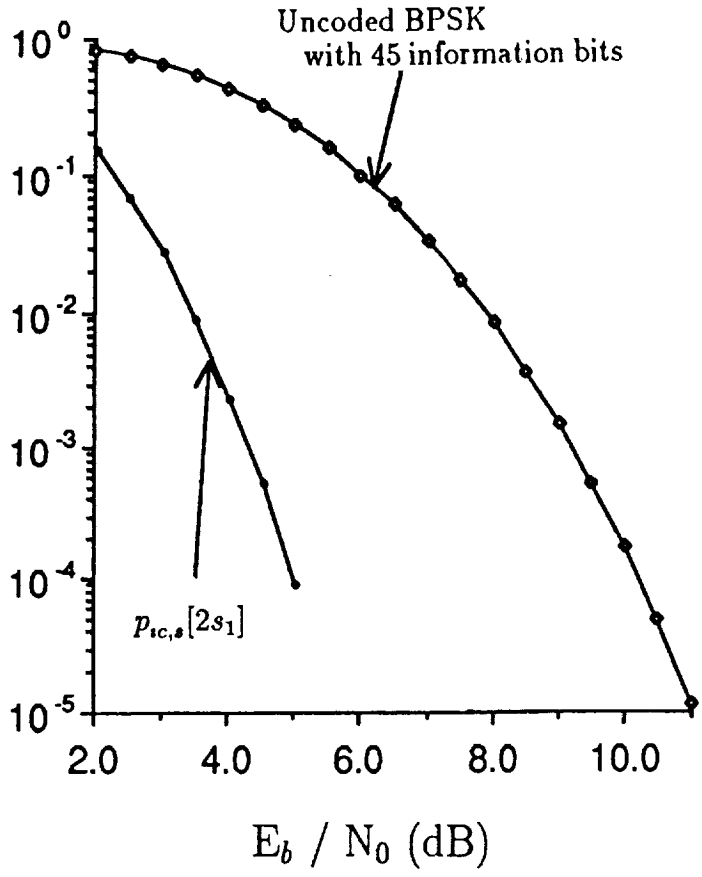

Figure 3. Error performance of extended and permuted (64,45)BCH